Итак, выбор функции энергии оказывает существенное влияние на визуально воспринимаемое качество изображения, полученного в результате непропорционального масштабирования. Очевидно, что для программных пакетов, предполагающих профессиональное использование, имеет смысл реализовать поддержку выбора функции энергии. Использование платформы параллельного программирования CUDA позволяет ускорить выполнение операции непропорционального масштабирования более чем в 15 раз.

Список литературы: 1. *Avidan S.* Seam carving for content-aware image resizing / *S. Avidan, A. Shamir* //ACM Trans. Graph., 2007. – Vol. 26, № 3. **2.** *Яне Б.* Цифровая обработка изображений / *Б. Яне*. – М.: Техносфера, 2007. – 584 с. **3.** *Боресков, А.В.* Основы работы с технологией CUDA / *А. В. Боресков, А. А. Харламов.* – М.: ДМК Пресс, 2010. – 232 с.

Поступила в редколлегию 01.06.2011

УДК 004.056.5

Е. Ю. ЛЕБЕДЕВА, ст. препод. кафедры ИУЗИС ОНПУ, г. Одесса;
Ю. Ф. ЛЕБЕДЕВ, начальник ИЦ НИИ Шторм, г. Одесса

ИССЛЕДОВАНИЕ МЕТРИК ИСПОЛЬЗУЕМЫХ ПРИ ОБНАРУЖЕНИИ КЛОНИРОВАННЫХ УЧАСТКОВ ИЗОБРАЖЕНИЙ В ЗАДАЧАХ ВЫЯВЛЕНИЯ ФАЛЬСИФИКАЦИИ

Досліджуються метрики для оцінки схожості блоків цифрового зображення, що використовуються в методі виявлення клонованих ділянок зображень при виявленні фальсифікації. Робляться виводи про доцільність вживання розглянутих метрик і виборі переважної метрики в умовах даного завдання.

Исследуются метрики для оценки схожести блоков цифрового изображения, используемые в методе обнаружения клонированных участков изображений при выявлении фальсификации. Делаются выводы о целесообразности применения рассмотренных метрик и выборе предпочтительной метрики в условиях рассматриваемой задачи.

Metrics are investigated for the estimation of blocks similarity of digital image, using in a detection method of the cloned areas of images when exposing the forensics. Drawn conclusion about using expedience of the considered metrics and choice of preferable metric in the conditions of the examined task.

Введение. Информация играет важную роль в человеческом обществе. Современные технологии позволяют хранить и обрабатывать информацию в цифровом виде. Появление быстродействующей компьютерной техники, современных цифровых камер и программного обеспечения, позволяющего обрабатывать цифровую информацию, привело к широкому распространению цифровой фальсификации.

Объектами фальсификации могут служить цифровые изображения (ЦИ) и цифровое видео (ЦВ). Фальсификации ЦИ и ЦВ зачастую нельзя обнаружить человеческим глазом. Учитывая, что ЦИ и ЦВ могут выступать доказательствами в работе правоохранительных органов и судов, чрезвычайно актуальным является решение проблемы выявления фальсификации в ЦИ и ЦВ.

Постановка задачи и цель исследования. Существует достаточно много способов создания фальсификации в ЦИ. Эти способы можно свести, например, в следующие группы [1]:

- Композиция (compositing). Два или более ЦИ сращиваются вместе и образуют композиционное изображение.
- Морфинг (morphing). Трансформация одного ЦИ в другое.
- Ретуширование (re-touching). В ЦИ вносится ряд программных вмешательств, таких как размытие (blur), смазывание (smudge) и клонирование частей изображения.
- Усиление (enhancing). В ЦИ вносится ряд изменений, таких как усиление или уменьшение резкости (sharpen), изменение цвета и контраста (color and contrast adjustment).
- Компьютерная графика (computer graphics). Изменяются ЦИ, которые были созданы с использованием графических программ, например, Autodesk 3ds Max.

В настоящей работе рассматриваются фальсификации, созданные путем клонирования частей одного и того же изображения, так как этот вид фальсификации очень часто используется ввиду легкости осуществления. Целью работы является исследование различных метрик и выбор наилучшей из них для обнаружения клонированных участков в ЦИ (ЦВ), не подвергшихся процедуре сжатия. Для решения поставленной цели необходимо решить следующие задачи:

1. Разработать методику обнаружения дублированных участков в изображении.
2. С учетом разработанной методики на основании вычислительного эксперимента проанализировать в качестве основного параметра, определяющего сходство между частями тестируемого изображения, различные метрики.
3. Выбрать предпочтительную метрику для решения рассматриваемой задачи используемым методом.

Метод обнаружения клонированных участков. Для обнаружения клонированных участков в задачах фальсификации предлагается следующая методика. Пусть имеется изображение I размера $M \times N$. Построим разбиение изображения на непересекающиеся блоки $D = \{d_1, d_2, \mathbf{K}, d_l\}$ размера $p \times p$ и на пересекающиеся блоки $C = \{c_1, c_2, \mathbf{K}, c_s\}$ размера $p \times p$, где $p < M$ и $p < N$. Необходимо найти для каждого блока $d_i, i = 1, \mathbf{K}, l$ подобный блок $c_j, j = 1, \mathbf{K} s$, т.е. $Metrica(d_i, c_j) = \delta$, где δ – некоторая

числовая константа. Если такой блок найден, например d_i и c_j, то эти блоки помечаются как дублированные. Объединение дублированных блоков $\mathbf{U} d_k, k \le l$, $\mathbf{U} c_f, f \le s$ и определяет возможные клонированные части изображение I.

Возникает вопрос, какие метрики можно использовать в качестве меры подобия блоков $Metrica(d_i, c_j)$.

Обзор метрик для определения подобия блоков. Рассмотрим несколько наиболее известных метрик для определения подобия блоков в изображении I, таких как MSE, коэффициент корреляция, расстояние Минковского и HS [2]. Для вычисления метрик преобразуем изображения из цветовой модели RGB в YUV.

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.522 & 0.311 \end{bmatrix} \cdot \begin{bmatrix} R \\ G \\ B \end{bmatrix}., \quad (1)$$

Модель YUV (1) основана на разложении изображения на три составляющие: Y – самая значимая составляющая определяющая яркость точки изображения; U, V – две цветовые составляющие (их называют цветоразностями, т.к. U = G – R, V = G – B).

При работе с метриками будем использовать только составляющую Y.

Наиболее простой метрикой является среднеквадратичная ошибка MSE (mean squared error):

$$MSE = \frac{1}{p \times p} \sum_{rt} (d_{rt} - c_{rt})^2, \quad (2)$$

где d_{rt}, c_{rt} – значения яркости каждого пикселя блока.

Коэффициент корреляции указывает силу связи между исследуемыми объектами [3]. Рассмотрим коэффициент корреляции Пирсона:

$$R = \frac{\sum_{rt} \left(d_{rt} - \overline{d_{rt}}\right)\left(c_{rt} - \overline{c_{rt}}\right)}{\sqrt{\sum_{rt} \left(d_{rt} - \overline{d_{rt}}\right)^2 \sum_{rt} \left(c_{rt} - \overline{c_{rt}}\right)^2}}, \quad (3)$$

где $\overline{d_{rt}}, \overline{c_{rt}}$ – среднее значения яркости блока.

Степенное расстояние Минковского, является обобщенным выражением Евклидового расстояния:

$$M = \left(\sum_{rt} |d_{rt} - c_{rt}|^p \right)^{\frac{1}{p}}, \quad (4)$$

где p – произвольное целое число.

Метрика Histogram Similarity (HS) вычисляется по результатам построения гистограммы по блоку изображения (5). Гистограмма — это график распределения полутонов изображения, в котором по горизонтальной оси представлена яркость, а по вертикали — число пикселей блока изображения с данным значением яркости.

$$HS = \sum_{y=0}^{255} \left| f_{d_i}(y) - f_{c_j}(y) \right|, \quad (5)$$

где $f_{d_i}(y)$, $f_{c_j}(y)$ – значения гистограммы для блоков d_i и c_j соответственно.

Результаты исследований. Для исследований возьмем изображения, полученные с помощью цифрового фотоаппарата. Клонированные участки добавлены с помощью программы Adobe Photoshop CS. Результаты фальсификации не подвергались сжатию (рис. 1). Использовалось разбиение изображения на блоки размера 8×8 пикселей.

Рис. 1 – Исходные изображения (слева) и фальсифицированные (справа)

К каждому фальсифицированному изображению в качестве меры подобия блоков применили рассмотренные выше метрики. Помечаем блоки как дублируемые, если значение метрик MSE (2), расстояние Минковского

(4), HS (5), равно нулю, а значение коэффициента корреляции (3) равно 1. Найденные дублируемые блоки помещаются в результирующее изображение в те позиции, где они были обнаружены. Результаты применения метрик, в обнаружении клонированных участков представлены на рисунке 2.

Из представленных результатов можно заметить, что все рассмотренные метрики определяют практически точно клонированные участки.

Для получения более точной границы клонированных участков необходимо использовать разбиение на блоки меньших размеров, что в свою очередь может привести к появлению лжеблоков. Для ускорения работы метода целесообразно разбивать изображение на блоки больших размеров, что в свою очередь может ослабить точность обнаружения границ клонированных участков, а также может привести к не выявлению таковых.

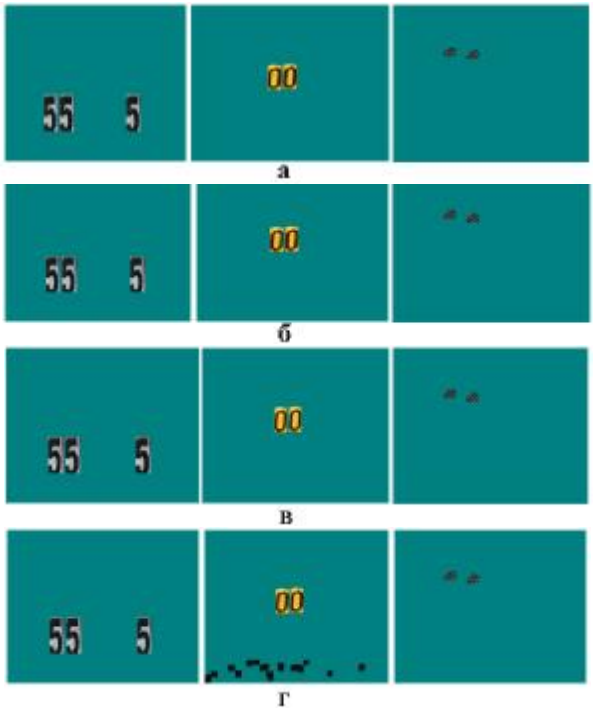

Рис. 2 – Результаты работы метрик: *а* – MSE; *б* – коэффициента корреляции; *в* – расстояния Минковского; *г* – Histogram Similarity

Следующим этапом наших исследований является выяснение, какие значения принимают метрики рядом с обнаруженными дублирующими

участками. Это позволит экспериментальным путем выявить порог, который позволит дополнительно обрабатывать те блоки, значение метрик которых соответствуют установленному пороговому значению. Под обработкой в этой ситуации понимаем деление блока на подблоки меньших размеров. Рассмотрим, как распределяются значения метрик для второго фальсифицированного изображения рядом с найденными дублирующими блоками (рис. 3). В случае метрик MSE, расстояние Минковского и HS фиксируется минимальное значение метрики для текущего блока d_i. Для коэффициента корреляции – максимальное значение.

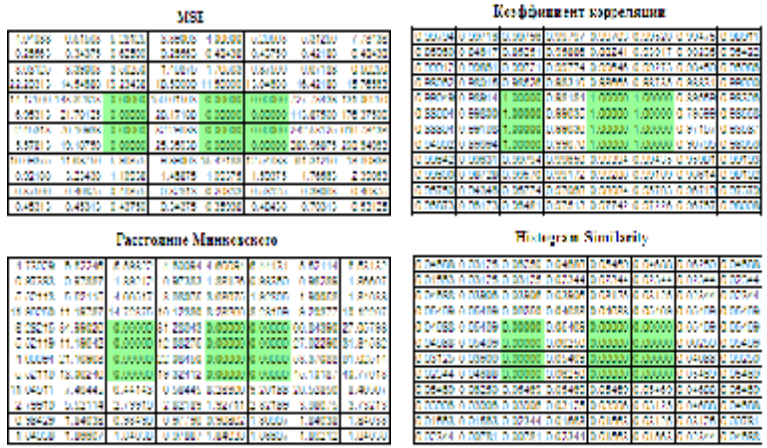

Рис. 3 – Распределение значений метрик возле дублирующих участков (дублирующиеся участки обозначены закрашенным фоном)

Для получения более точной границы дублирующихся участков, следует рассмотреть блоки окружающие найденные или находящиеся между ними. Эти блоки могут содержать в себе части фальсификаций, которые можно будет обнаружить, разбив их на более мелкие. Для автоматизации процесса уточнения границ участков фальсификации, необходимо подобрать такое пороговое значение, появление которого было бы маловероятно в других блоках изображения, не содержащих частей дублирующихся участков. По полученным результатам (рис. 3) можно увидеть, что метрики MSE, расстояние Минковского и HS не подходят для такого уточнения.

Выводы. Предложенная методика, использующая в качестве параметра коэффициент корреляции, позволяет точно обнаружить местоположение клонированных участков изображения. Хотя все рассмотренные метрики одинаково фиксируют дублирующиеся блоки, но для последующего уточнения наиболее предпочтительным является коэффициент корреляции, так как экс-

периментальным путем для него можно получить универсальное пороговое значение, позволяющее более точно определить границы клонированных участков.

Список литературы: **1.** *Alin C. Popescu* Statistical Tools for Digital Image Forensics / *Alin. C. Popescu* // Phd Thesis Dartmouth College. – 2004. – P. 131. **2.** *M. Kutter* A fair benchmark for image watermarking systems / *M. Kutter, F. A. P. Petitcolas* // Electronic Imaging '99. Security and Watermarking of Multimedia Contents. – 1999. – vol. 3657. – P. 226–239. **3.** *Гмурман В. Е.* Теория вероятностей и математическая статистика / *В. Е. Гмурман* . – М. : Высшая школа, 2004. – 479 с.

Надійшла до редколегії 07.06.2011

УДК 004.056

В. В. ЗОРИЛО, аспирант ОНПУ, г. Одесса

ВЫЯВЛЕНИЕ КЛОНИРОВАНИЯ КАК ФАЛЬСИФИКАЦИИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

Розроблено та програмно реалізовано метод, який дозволяє виявити та локалізувати фальсифікацію цифрового зображення, проведену за допомогою інструменту «Штамп», реалізованого у більшості графічних редакторів. Розроблений метод значно перевершую аналогів з швидкодії.

Разработани программно реализован метод, позволяющий выявить и локализовать фальсификацию цифрового изображения, проведенную с помощью инструмента «Штамп», реализованного в большинстве графических редакторов. Разработанный метод значительно превосходит аналоги по быстродействию.

The detection digital image falsification method is developed and implemented. The falsification made by using Adobe Photoshop instrument "Clone". These methods calculate complicity is much less than this one parameter in other similar methods.

Введение. В век глобальной компьютеризации и интенсивного развития информационных технологий особенно остро ставится вопрос защиты информационных систем. Вместе с информационными технологиями развивается и компьютерная преступность, используя для своих противозаконных действий все более изощренные методы. В частности, такой вид компьютерной преступности, как подделка информации, может преследовать различные цели. Итогом подделки является то, что потребителю информации будут предоставлены недостоверные данные. Примером могут служить подтасовка результатов выборов или же хищение различного вида товаров путем ввода в программу фальшивых данных; подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков; изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов.

Ежегодно на борьбу с киберпреступностью развитые страны мира выделяют миллионы долларов. Новые компьютерные атаки требуют постоянного развития методов защиты информации. Практически во всех областях нашей жизни (медицина, охранные системы, системы безопасности, судебные разбирательства) используются цифровые аудио-, видео-, изображения. Их подделка доступна всем компьютерным пользователям. Чаще всего фальсификации подвергаются цифровые изображения (ЦИ). Ввиду этого особенно *актуальным* на сегодняшний день является умение отличить подделку от подлинного сигнала. В [1] была разработана общая методология анализа свойств, состояния и технологии функционирования произвольной информационной системы, которая успешно адаптируется для решения вопросов, связанных с идентификацией фальсификаций цифровых сигналов [2, 3].

В данной работе продолжается исследование возможностей обнаружения несанкционированного изменения цифрового сигнала, в частности, фотомонтажа ЦИ, и разработка методов решения этой актуальной проблемы.

Постановка проблемы и цель исследования. Из практики известно, что наиболее часто при подделке фотографий необходимо убрать какой-то предмет, либо, наоборот, продублировать его. В Adobe Photoshop для решения этой задачи чаще всего, если не всегда, применяют инструмент «Штамп». Данный инструмент используется для переноса клона объекта из одной части изображения в другую путем параллельного переноса, как правило, в пределах одной и той же фотографии. Как нам известно из открытой печати, наиболее успешным методом обнаружения такой фальсификации является метод, основанный на корреляции коэффициентов дискретного косинусного преобразования матрицы изображения [4], однако данный метод в реальных условиях требует значительных вычислительных затрат. Как показано в [2], любое вмешательство в ЦИ отразится на сингулярных числах (СНЧ) его матрицы и приведет к некоторым их особенностям. Выявление таких особенностей даст возможность отличить подлинное изображение от подвергнутого обработке штампом, что, в свою очередь, в случае наличия фальсификации позволит не использовать исследуемое ЦИ, например, в качестве доказательства чего-либо в суде. *Целью* данной работы является разработка метода выявления фальсификации цифрового изображения, выполненной посредством инструмента «Штамп» в Adobe Photoshop. Для достижения поставленной цели необходимо решить следующие задачи:

- выделить и обосновать целесообразность математических параметров, определяющих ЦИ, являющихся объектом сравнения при поиске клонированных участков;
- выявить характерные особенности математических параметров, определяющих изображение, при различных форматах хранения: с потерями и без потерь;
- разработать практический метод отделения ЦИ, подвергавшегося обработке штампом, от изображения, которое не подвергалось данной операции; реализовать его программно;